(19) JAPANESE PATENT OFFICE

PATENT ABSTRACTS OF JAPAN

(11) Publication number: **10143493 A**

(43) Date of publication of application: **29 . 05 . 98**

(51) Int. Cl **G06F 17/10**
G09C 1/00
H03M 7/50

(21) Application number: **08336202**

(22) Date of filing: **13 . 11 . 96**

(71) Applicant: **SEIBU:KK**

(72) Inventor: **SHONO KATSUFUSA**
AKIYAMA MUNEYUKI

(54) **TIME SERIES FOR CHAOS**

(57) Abstract:

PROBLEM TO BE SOLVED: To make chaos industrially practicable by matching a square quantum size by nonlinearly performing quantization processing to a nonlinear function.

SOLUTION: At the time of nonlinearly quantizing the linearly quantized time series of the internal state of the chaos again, inclination is obtained for all input corresponding to the quantums of an equal size on the input/output transmission characteristics of linear quantization, classification is performed corresponding to the inclination, re-classification is performed by a threshold value processing based on defined weight, normalization is performed, bundling is newly performed and the quantization is performed. By taking out the square quantums of the matched quantum size without ov'erlap on the graph of the transmission characteristics along a 45 degree line, allocating a blocked digital code and attaining an input code, a cipher restoration system utilizing the chaos is made designable. The allocation of the input code without the localization of distribution is made possible and the internal state of the chaos is effectively utilized.

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平10－143493

(43)公開日　平成10年(1998)５月29日

(51)Int.Cl.[6]	識別記号	ＦＩ	
Ｇ０６Ｆ　17/10		Ｇ０６Ｆ　15/31	Ｚ
Ｇ０９Ｃ　1/00	６１０	Ｇ０９Ｃ　1/00	６１０Ｚ
Ｈ０３Ｍ　7/50		Ｈ０３Ｍ　7/50	

審査請求　未請求　請求項の数１　書面　（全　４　頁）

(21)出願番号　特願平8－336202

(22)出願日　平成８年(1996)11月13日

(71)出願人　596180995
株式会社セイブ
佐賀県西松浦郡有田町西部甲753

(72)発明者　庄野　克房
神奈川県横浜市旭区白根５丁目45番12号

(72)発明者　秋山　宗志
佐賀県西松浦郡有田町中樽３丁目５番15号

(54)【発明の名称】　カオスのタイムシリーズ

(57)【要約】

【目的】　非線形一次写像回路の生成するカオスのタイムシリーズを非線形に束ねなおして量子化し、伝達特性の中に見出される１対多又は多対１の関係を産業に利用する。

【構成】　線形に量子化して計測したカオスのタイムシリーズの入出力伝達特性上で傾斜を求め、傾斜に応じた重みで非対象に束ねなおすことにより非線形に量子化しなおしたタイムシリーズを用い、ディジタルデータの検索を行い過去に戻った複数の状態への変換とその逆変換を利用する電子情報通信分野におけるディジタル情報処理技術である。

【特許請求の範囲】

【請求項１】　線形に量子化したカオスの内部状態のタイムシリーズを非線形に量子化しなおすにあたって、線形量子化の入出力伝達特性上において等しいサイズの量子に対応する全ての入力について傾斜を求め、傾斜に応じた分類をし、定義された重みにもとづくしきい値処理により再分類をするとともに正規化をしてあらためて束ねなおし量子化したことを特徴とするカオスのタイムシリーズ。

【発明の詳細な説明】

【０００１】

【産業上の利用分野】本発明はカオス発生回路が生成するカオスの内部状態ｙ（ｔ）（ｔは離散時間、ｔ＝０，１，２，…）の作るタイムシリーズｙ（ｔ）－ｔの量子化手法に関する。

【０００２】従来のエレクトロニクス産業は１対１対応関係のもとで明確な因果関係にのみしたがって構築されてきた。一方、非線形一次元写像回路の生成するカオスには、その過去には分岐を生じ、将来には発散と収束を＊繰り返す。１対多及び多対１の対応関係を内蔵し、新しい産業の可能性を与える。

【０００３】１対多の関係は暗号コードの生成に、多対１の関係は暗号コードの復元に利用される。

【０００４】多対１の関係は画像や音声データの圧縮に利用され、１対多の関係を利用して再生展開される。

【０００５】

【従来の技術】増加関数を与える電子回路と減少関数を与える電子回路の入力および出力を共通にした並列接続により関数合成を行う一次元写像回路を、ＣＭＯＳスイッチを介してフリップフロップのループに構成することにより、カオス発生回路が実現される。そのとき、カオス発生回路の入出力伝達特性が解析的な関数関係で記述できるわけではない。

【０００６】分解能１６ビットのＡＤＣ（アナログ・ディジタル変換器）でカオス発生回路の内部状態ｙ（ｔ）を計測したとする。ｙ（ｔ）は０～６５５６３の量子（整数）のいづれかに属する。初期値ｙ（Ｏ）は０～６５５６３の量子の一つである整数で与えられる。１６ビット汎用ＡＤＣで線形に量子化した内部状態を$y_{16}(t)$と書くと、$0 \leq y_{16}(t) \leq 65563$である。電子回路の合成関数が与える一次元写像関数一次元写像関数ｆにより生成されるカオスの伝達特性は

$$y_{16}(t+1) = f\{y_{16}(t)\} \qquad (1)$$

により入力$y_{16}(t)$と出力$y_{16}(t+1)$の関係として与えられる。

【０００７】カオスのタイムシリーズ$y_{16}(t)-t$を離散時間ｔに沿って検索し、$y_{16}(t)$を発見したらτステップ過去に戻った値$y_{16}(t-\tau)$、あるいはτステップ将来の値$y_{16}(t+\tau)$も求めることができ、入力$y_{16}(t)$に対する出力$y_{16}(t-\tau)$あるいは$y_{16}(t+\tau)$の関係が求められる。

【０００８】カオスの過去には分岐を生ずるので、$y_{16}(t-\tau)$は複数の異なる整数値となる。将来には決定論的に状態が決まるが発散と収束を繰り返すので、$y_{16}(t-\tau)$は整数値の幅を持った値となる。

【０００９】$y_{16}(t)$から出発し過去へτステップ戻り、再びτステップ将来へ進んだ値を$y_{16}(t-\tau+\tau)$と記すと、$y_{16}(t)$と$y_{16}(t-\tau+\tau)$は往復した伝達特性となる。$y_{16}(t)$を横軸にとり$y_{16}(t-\tau+\tau)$を縦軸にとったグラフは、４５度線に沿って正方形が並ぶことになる。非線形関数ｆの伝達特性を線形に量子化して計測したとき、量子サイズが様々となり、往復した伝達特性の正方形のサイズは様々で相互に重なり合う。

※【００１０】カオスの応用、たとえば暗号化復元システムを設計するとき、量子サイズが不揃いだと、カオスの内部状態を平等に有効利用することが難しい。本発明は、非線形関数を非線形に量子化処理を行うことにより、正方形の量子サイズをそろえ、カオスの工業的実用化に道を開くものである。

【００１１】

【課題を解決するための手段】線形に計測したタイムシリーズ、たとえば$y_{16}(t)-t$を非線形に束ねなおすことにより量子サイズをそろえる処理のアルゴリズムは以下の通りである。関数ｆは計測はされるが、解析的に関数関係で記述できないので、非線形処理は数値的に行われる。

【００１２】すべての$y_{16}(t)$に関し、傾斜$df/dy_{16}(t)$を求める。

【００１３】$df/dy_{16}(t)$が、たとえば２より大きい$y_{16}(t)$には重みとしてｗ＝１．５を与え、$df/dy_{16}(t)$が２より小さい$y_{16}(t)$には重みとしてｗ＝１．０を与える。すなわち傾斜２をしきい値として、２以上の傾斜を緩くするように重みを与える。

【００１４】１６ビット線形量子化の内部状態$y_{16}(t)$を８ビット非線形量子化の内部状態$y'_{8}(t)$に束ねなおす場合を考える。次式にしたがって正規化した重み$w'\{y_{16}(t)\}$を求める。

$$w'\{y_{16}(t)\} = \frac{w\{y_{16}(t)\}}{\sum_{y_{16}(t)=0}^{65563} w\{y_{16}(t)\}} \qquad (2)$$

【００１５】次の式を満足するように８ビット非線形量子化の境界Ｂ（ｑ）をもとめる。

$$\sum_{y_{16}(t)=0}^{B(q)} w'\{y_{16}(t)\} = \frac{q+1}{2^8}$$

ここでｑは０，１，２，・・・・，２５５であり、Ｂ（２５５）＝６５５６３である。

【００１６】以上の非線形区分を、線形１６ビットから非線形８ビットに変換した例に限らず、一般化すること＊は容易である。また、上記の非線形区分処理を複数回繰り返しても効果がある。

【００１７】【作用】分解能８ビットに非線形量子化し、量子サイズをそろえたタイムシリーズｙ′ ｓ（ｔ）－ｔの中には１対多または多対１の伝達特性が見出される。

【００１８】タイムシリーズを離散時間ｔに沿って検索することにより、発見された$y'_8(t)$に対しτステップ過去に戻った内部状態の値$y'_8(t-\tau)$は複数個存在する。理想的には2^{τ}個発見される。$y'_8(t)$を入力コードとするとき、複数個発見される$y'_8(t-\tau)$は暗号コードとするのにふさわしい。複数個のうちどれが現れるかは確率によって決まり、予測することは難しい。

※　※【００１９】離散時間ｔを検索し、暗号コード$y'_8(t-\tau)$を発見したらτステップ将来へ進み$y'_8(t-\tau+\tau)$を見出すことができる。$y'_8(t-\tau+\tau)$は、入力コード$y'_8(t)$を含むが、発散のためにある幅を持って広がっている。その広がりは、理想的には2^{τ}ビットである。

【００２０】$y'_8(t)$から$y'_8(t-\tau+\tau)$を見たときの往復した伝達特性上では、45度線上に、理想的には2^{τ}ビット巾の正方形が$2^{8-\tau}$個等間隔に配置される。たとえば、τ＝４とすると2^4＝１６ビット巾の正方形の量子が１６個配置される。

【００２１】【実施例】通信線を介して電送されるディジタルコード列を暗号化復元するシステムについて実施例を述べる。

【００２２】１６個の正方形には、文字、画像、音声などの４ビットディジタルコード１６個を対応させて割り当てる。この割り当ての組み合わせは有効な暗号鍵である。その組み合わせの種類は１６！＝２．０９×１０★^{13}通りである。十分使い捨て可能な数の暗号鍵が用意できる。

【００２３】τを大きく選ぶと、暗号コードの種類は増えるが、定義できる入力コードの数は減少する。τを小さく選ぶと、暗号コードの種類は減るが、定義できる入力コードの数は増大し、暗号鍵の組み合わせの数は指数関数的に増大する。

【００２４】文字、画像、音声などのディジタルコードを４ビット単位にブロック化しタイムシリーズ$y'_8(t)-t$上で暗号化復元を行った場合、ペンティアム 133 MHz CPU及び３２Mバイトメモリを用いたとき、暗号化処理速度１１．６ｋバイト／秒、また復元処理速度１６．７ｋバイト／秒が達成された。

【００２５】暗号化処理は任意の離散時間ｔからの検索☆を保証する必要があるが、復元処理ではタイムシリーズをテーブル化して処理速度の高速化を計ることができる。

【００２６】より高速な暗号化を実現するためには、タイムシリーズ$y'_8(t)-t$を、離散時間ｔを残してハッシュテーブル化することである。この手法を採用することにより、４ビット単位にブロック化したとき最高２Mバイト／秒の暗号化処理速度が実現できた。８ビット量子化のタイムシリーズでτ＝４と選んだ本実施例は理解しやすい１例にすぎない。１６ビット量子化のタイムシリーズでτ＝８とし８ビット単位でブロック化するなど、実際の工業的利用にあたっては一般化して実施されることは当然である。

【００２７】暗号化復元は１対多から多対１への変換を利用した実施例であるが、多対１対応をデータ圧縮過程に利用し、１対多対応を圧縮データの展開再生に利用して画像や音声データの圧縮転送を実現することができる。

【００２８】【発明の効果】以上、実施例を用いて詳しく説明したように、一次元写像を用いたカオスの内部状態を、たとえば汎用ＡＤＣで線形に計測して一連のタイムシリーズｙ（ｔ）－ｔを求め、量子サイズをそろえるように束ねなおす数値処理のアルゴリズムが具体的に示された。タイムシリーズ上を往復した伝達特性ｙ（ｔ）－ｙ（ｔ－τ＋τ）のグラフ上で、量子サイズのそろった重なりのない正方形の量子が４５度ラインに沿って取り出され、ブロック化したディジタルコードを割り当てて入力コードとすることにより、カオスを利用した暗号化復元システ

ムが設計可能となる。分布にかたよりのない入力コードの割り当てが可能となり、カオスの内部状態を有効利用＊＊できるようになった。本発明の電子情報通信産業における情報の安全管理に寄与する効果は顕著である。